

- 32 -

ABSTRACT OF THE DISCLOSURE

A system for providing intrusion detection in a network wherein data flows are exchanged using associated network ports and application layer protocols. The system includes a monitoring module configured for monitoring data flows in the network, a protocol identification engine configured for detecting information on the application layer protocols involved in the monitored data flows, and an intrusion detection module configured for operating based on the information on application layer protocols detected. Intrusion detection is thus provided independently of any predefined association between the network ports and the application layer protocols.